

Received & Inspected  
MAR 2 2009  
FCC Mail Room

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: February 16, 2009

Name of company(s) covered by this certification: East Otter Tail Telephone Company, Callaway Telephone Company, Twin Valley-Ulen Telephone Company, Tekstar Communications, Inc., Royale Comtronics, Inc., Midwest Telephone Co., Osakis Telephone Company and The Peoples Telephone Co. of Bigfork all of Minnesota d.b.a. Arvig Communications Systems.

Form 499 Filer ID: 811492, 806904, 803133, 803130, 825278, 803466, 804774, 819354

Name of signatory: Richard Vyskocil

Title of signatory: Treasurer

I, Richard Vyskocil, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed

  
Company Officer

No. of Copies rec'd  
List ABCDE

044

## STATEMENT OF COMPLIANCE

The operating procedures of East Otter Tail Telephone Company, Callaway Telephone Company, Twin Valley-Ulen Telephone Company, Tekstar Communications, Inc., Royale Comtronics, Inc., Midwest Telephone Company, Osakis Telephone Company, The Peoples Telephone Company of Bigfork ensure compliance with the FCC's CPNI Rules. Such procedures are as follows:

### *Use of CPNI in Marketing*

Before (but proximate to) soliciting customer consent for the use of CPNI to market either (a) our (or our affiliates') communication-related services; or (b) third-parties' communication-related services, we give each customer notice of his or her right to restrict use and disclosure of, and access to, his or her CPNI, in compliance with FCC Rule 64.2008. Our company maintains a record of these notifications for at least one year.

Our company accesses and uses a customer's CPNI to market our own (or our affiliates') communication-related services (outside a customer's current relationship) only after the customer's Opt-Out consent has been obtained in compliance with FCC Rule 64.2008, and which consent has not been revoked by the customer. Every two years our company (a) provides notice of customers' rights to restrict use and disclosure of, and access to, their CPNI, in compliance with FCC Rule 64.2008, and (b) solicits Opt Out consent for the use of the customer CPNI, in compliance with FCC Rule 64.2008, to each customer who has given Opt Out consent.

Our company has implemented a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI. Each customer's record contains a designation identifying whether or not we have obtained, through the processes permitted by the FCC's rules, the customer's approval to use, disclose or permit access to his or her CPNI.

Our company has a supervisory review process regarding our compliance with the FCC's CPNI rules for any outbound marketing efforts. We require sales personnel to obtain supervisory approval of any proposed outbound targeted marketing request for customer approval.

### *CPNI Safeguards*

Our company has designated a compliance officer to maintain and secure the company's CPNI records and to supervise training of all company employees.

Our company trains its personnel as to when they are, and are not, authorized to use or disclose CPNI, and we have a disciplinary process in place if the rules are violated.

Our company authenticates the identity of a customer; a password may be used, prior to disclosing CPNI based on a customer-initiated telephone contact, online account access, or in-store visit.

Our company discloses call detail information (CDI) in only one of these three ways; by sending the CDI to the customer's address of record via USPO; or provides the information after the customer has presented two forms of ID in person (one form begin a valid picture ID that matches the account information); or provides the information to local law enforcement in person or in response to a subpoena.

Our company discloses CPNI to a customer in person at our retail location(s) only when the customer presents a valid photo ID and the ID matches the name on the account.

Our company has established password protection for customers' online accounts. Neither passwords nor the backup method for authentication rely on customers' readily available biographical information.

Our company notifies a customer immediately of changes in: a customer's password, a customer's response to back-up means of authentication, online account, or address of record.

### ***CPNI Recordkeeping and Reporting***

Our company maintains a record of our own and our affiliates' sales and marketing campaigns that use customer CPNI. We maintain these records for at least one year.

Our company is prepared to provide the FCC with written notice, within five business days of any instance where the "opt out" mechanisms do not work properly.

Our company is prepared to notify the U.S. Secret Service and FBI within seven business days after the occurrence of an intentional, unauthorized (or exceeding authorization), access to, use of, or disclosure of CPNI. We may also notify the customer of such breach, after consulting with the investigatory agency(ies), if we believe there is an extraordinarily urgent need to notify a customer (or class of customers) in order to avoid immediate or irreparable harm. We will notify the customer of the breach after 7 business days following notification to the FBI and Secret Service, if such agencies have not requested that we postpone disclosure to the customer.

Our company will maintain records of any discovered breaches, notices to the Secret Service and FBI, and their responses, for at least two years.